A Simple Derivation for the Frobenius Pseudoprime Test

Daniel Loebenberger

b-it
Universität Bonn
D53113 Bonn
daniel@bit.uni-bonn.de

Abstract. Probabilistic compositeness tests are of great practical importance in cryptography. Besides prominent tests (like the well-known Miller-Rabin test), there are tests that use Lucas-sequences for testing compositeness. One example is the so-called Frobenius test that has a very low error probability. Using a slight modification of the above mentioned Lucas sequences we present a simple derivation for the Frobenius pseudoprime test in the version proposed by Crandall and Pomerance in [CrPo05].

1 Lucas and Frobenius Pseudoprimes

For \( f(x) = x^2 - ax + b \in \mathbb{Z}[x] \) the Lucas sequences are given by

\[
U_j := U_j(a, b) := \frac{x^j - (a - x)^j}{x - (a - x)} \pmod{f(x)} \\
V_j := V_j(a, b) := x^j + (a - x)^j \pmod{f(x)}
\]  

These sequences both satisfy the same recurrence relation

\[
U_j = aU_{j-1} - bU_{j-2} ; \quad V_j = aV_{j-1} - bV_{j-2} \quad \text{for } j \geq 2
\]

with initial values

\[
U_0 = 0, \quad U_1 = 1 \quad V_0 = 2, \quad V_1 = a
\]

The following theorem is the basis for a probabilistic prime test, called the Lucas test:

**Theorem 1.** Let \( a, b \in \mathbb{Z} \setminus \{0\} \), \( \Delta := a^2 - 4b \) and the sequences \( (U_j), (V_j) \) defined as above. If \( p \) is prime, with \( \gcd(p, 2ab\Delta) = 1 \), we have:

\[
U_{p-\frac{\Delta}{2}} \equiv 0 \pmod{p}
\]

**Proof.**

If \( \Delta \) is a quadratic nonresidue modulo \( p \), then the polynomial \( f(x) \in \mathbb{Z}_p[x] \) is irreducible over \( \mathbb{Z}_p \), which means that \( \mathbb{Z}_p[x]/(f(x)) \) is a field and isomorphic to \( \mathbb{F}_{p^2} \). The elements of the subfield \( \mathbb{Z}_p \) are exactly those elements \( i + jx \in \mathbb{Z}_p[x]/(f(x)) \) with \( j = 0 \).

The zeroes of the polynomial \( f(x) \) are \( x \) and \( a - x \), both in \( \mathbb{F}_{p^2} \setminus \mathbb{Z}_p \), and therefore permuted by the Frobenius automorphism. Thus we have

- in the case \( (\frac{\Delta}{p}) = -1 \):
  \[
  \begin{cases} 
  x^p \equiv a - x \pmod{f(x), p} \\
  (a - x)^p \equiv x \pmod{f(x), p}
  \end{cases}
  \]
which implies $x^{p+1} - (a - x)^{p+1} = x(a - x) - (a - x)x \equiv 0 \pmod{f(x), p}$, as claimed.

If, on the other hand, $\Delta$ is a quadratic residue modulo $p$, then $f(x) \bmod p$ has two roots in $\mathbb{Z}_p$ and $R := \mathbb{Z}_p[x]/(f(x))$ is isomorphic to the direct product $\mathbb{Z}_p \times \mathbb{Z}_p$. In this case the Frobenius automorphism acts trivially on $R$ and we have:

$$
\text{in the case } \left(\frac{\Delta}{p}\right) = 1 : \begin{cases} 
   x^p \equiv x \pmod{f(x), p} \\
   (a - x)^p \equiv a - x \pmod{f(x), p}
\end{cases}
$$

Since $\gcd(p, b) = 1$ and since $x(a - x) \equiv b \pmod{f(x), p}$, the elements $x$ and $a - x$ are units in $R$. Therefore we have $x^{p-1} = (a - x)^{p-1} = 1$ as desired.

**Definition 2.** Let $a, b \in \mathbb{Z} \setminus \{0\}$, with $\Delta = a^2 - 4b$ not a square. A composite integer $n$, with $\gcd(2ab\Delta, n) = 1$ is called a Lucas pseudoprime with respect to $f(x) := x^2 - ax + b$, if $U_{n-\left(\frac{\Delta}{n}\right)} \equiv 0 \pmod{n}$.

The first Lucas pseudoprime with respect to the Fibonacci-polynomial $x^2 - x - 1$ is $323 = 17 \cdot 19$.

Grantham proposed a stronger test, the *Frobenius test* (see [Gra98] and [Gra01]). The definition of the Frobenius pseudoprime is given by

**Definition 3.** Let $a, b \in \mathbb{Z} \setminus \{0\}$, with $\Delta = a^2 - 4b$ not a square. A composite integer $n$, with $\gcd(2ab\Delta, n) = 1$ is called a Frobenius pseudoprime with respect to $f(x) := x^2 - ax + b$, if

$$
x^n \equiv \begin{cases} 
   a - x \pmod{f(x), n} & \text{if } \left(\frac{\Delta}{n}\right) = -1 \\
   x \pmod{f(x), n} & \text{if } \left(\frac{\Delta}{n}\right) = 1
\end{cases}
$$

Next we show that the Frobenius pseudoprime test is at least as strong as the Lucas pseudoprime test:

**Theorem 4.** Let $f(x) := x^2 - ax + b$ and $n \in \mathbb{N}$. If $n$ is Frobenius pseudoprime with respect to $f(x)$, then $n$ is also Lucas pseudoprime with respect to $f(x)$.

Before we can prove this theorem we need the following lemma:

**Lemma 5.** Let $m, n \in \mathbb{N}$, $f(x), g(x), r(x) \in \mathbb{Z}[x]$. If $f(r(x)) \equiv 0 \pmod{f(x), n}$ and $x^m \equiv g(x) \pmod{f(x), n}$, then $r(x)^m \equiv g(r(x)) \pmod{f(x), n}$.

**Proof.** Clearly $x^m \equiv f(x)h(x) + g(x) \pmod{n}$ for $h(x) \in \mathbb{Z}[x]$. Since $x$ is a variable we also have $r(x)^m \equiv f(r(x))h(r(x)) + g(r(x)) \pmod{n}$. Because we have $f(r(x)) \equiv 0 \pmod{f(x), n}$, it follows $r(x)^m \equiv g(r(x)) \pmod{f(x), n}$.

Now the proof for Theorem 4 is easy:

**Proof.** Let $n$ be Frobenius pseudoprime with respect to $f(x)$, according to Definition 3.

Assume $\left(\frac{\Delta}{n}\right) = 1$. Then $x^n \equiv x \pmod{f(x), n}$. Since $\gcd(b, n) = 1$, $x$ modulo $(f(x), n)$ is invertible and we have $x^{n-1} \equiv 1 \pmod{f(x), n}$. Since $f(a - x) \equiv 0 \pmod{f(x), n}$ Lemma 5 implies the congruence $(a - x)^{n-1} \equiv 1 \pmod{f(x), n}$, i.e. $(a - x)^n \equiv (a - x) \pmod{f(x), n}$.

On the other hand, if $\left(\frac{\Delta}{n}\right) = -1$, we get from $x^n \equiv a - x \pmod{f(x), n}$ and $f(a - x) \equiv 0 \pmod{f(x), n}$ directly by Lemma 5 the congruence $(a - x)^n \equiv x \pmod{f(x), n}$ as desired.

Thus in both cases $n$ is Lucas pseudoprime with respect to $f(x)$.
The Frobenius property for quadratic polynomials can be expressed using the Lucas sequences $(U_j)$ and $(V_j)$:

**Theorem 6.** Let $a, b \in \mathbb{N}$, with $\Delta = a^2 - 4b$ not a square. An integer $n$, with $\gcd(2ab\Delta, n) = 1$ is Frobenius pseudoprime with respect to $f(x) := x^2 - ax + b$, if and only if

$$U_{n - \left(\frac{\Delta}{n}\right)} \equiv 0 \pmod{n} \text{ and } V_{n - \left(\frac{\Delta}{n}\right)} \equiv \begin{cases} 2b & \text{if } \left(\frac{\Delta}{n}\right) = -1 \\ 2 & \text{if } \left(\frac{\Delta}{n}\right) = 1 \end{cases}$$

(3)

**Proof.** From the definitions of the Lucas sequences (1) one easily sees, that

$$2x^j \equiv V_j + (2x - a)U_j \pmod{f(x)}$$

(4)

Assume (3). In the case $\left(\frac{\Delta}{n}\right) = -1$ Eqn. (4) implies $x^{n+1} \equiv b \pmod{f(x), n}$ and in the case $\left(\frac{\Delta}{n}\right) = 1$ Eqn. (4) gives $x^{n-1} \equiv 1 \pmod{f(x), n}$. The latter implies $x^n \equiv x \pmod{f(x), n}$, and since $x(a - x) \equiv b \pmod{f(x), n}$ the first leads to $x^{n} \equiv a - x \pmod{f(x), n}$. So $n$ is Frobenius pseudoprime.

On the other hand, if $n$ is Frobenius pseudoprime with respect to $f(x)$, we have $U_{n - \left(\frac{\Delta}{n}\right)} \equiv 0 \pmod{n}$ by Theorem 4. For $j = n - \left(\frac{\Delta}{n}\right)$ Eqn. (4) gives

$$2x^{n-\left(\frac{\Delta}{n}\right)} \equiv V_{n - \left(\frac{\Delta}{n}\right)} \pmod{f(x), n}$$

Assume $\left(\frac{\Delta}{n}\right) = -1$. Then Definition 3 gives $x^{n+1} \equiv (a - x)x \equiv b \pmod{f(x), n}$, i.e. $V_{n+1} \equiv 2b \pmod{n}$. Finally assume $\left(\frac{\Delta}{n}\right) = 1$. Since $x$ is invertible in $\mathbb{Z}_n[x]/(f(x))$, it follows $x^{n-1} \equiv 1 \pmod{f(x), n}$, i.e. $V_{n-1} \equiv 2 \pmod{n}$.

The first Frobenius pseudoprime with respect to the Fibonacci polynomial $x^2 - x - 1$ is 4181, the nineteenth Fibonacci number, the first with $\left(\frac{\Delta}{n}\right) = -1$ is 5777. Thus not every Lucas pseudoprime is a Frobenius pseudoprime. We conclude that the Frobenius test is more stringent than the Lucas test.

### 2 Efficient implementation

Suppose we want to apply the Frobenius test on a given number $n$. Choose $a, b \in \mathbb{N}$, with $\Delta = a^2 - 4b$ not a square such that $\gcd(2ab\Delta, n) = 1$.

Since $\gcd(2\Delta, n) = 1$ the number $n - \left(\frac{\Delta}{n}\right)$ is always even, say $n - \left(\frac{\Delta}{n}\right) = 2m$, $m \in \mathbb{N}$.

Following Williams [Wil98] we define the following modified Lucas sequence

$$W_j := b^{-1}V_{2j} \pmod{n}$$

(5)

Since $\gcd(b, n) = 1$ the sequence $(W_j) := (W_j)_{j \geq 0}$ is well defined and starts with

$$W_0 \equiv 2 \pmod{n} \text{ and } W_1 \equiv a^2b^{-1} - 2 \pmod{n}$$
The sequence \((W_j)\) can be computed efficiently. In fact, the following two formulas allow the computation of the values \(W_{2j}\) and \(W_{2j+1}\) from \(W_j\) and \(W_{j+1}\) \((j \geq 0)\):

\[
\begin{align*}
W_{2j} &\equiv W_j^2 - 2 \pmod{n} \\
W_{2j+1} &\equiv W_j W_{j+1} - W_1 \pmod{n}
\end{align*}
\] (6)

We arrive here at the novel, simple derivation for the Frobenius test:

**Proof.** Let \(\delta := x - (a - x)\), i.e.

\[
\delta^2 \equiv x^2 - 2b + (a - x)^2 \equiv a^2 - 4b \equiv \Delta \pmod{f(x), n}.
\]

Also, (1) has the consequence

\[
V_j + \delta U_j = 2x^j \quad \text{and} \quad V_j - \delta U_j = 2(a - x)^j.
\]

So we have for arbitrary \(j, k \in \mathbb{N}\)

\[
\begin{align*}
(V_j + \delta U_j) \cdot (V_k + \delta U_k) &= 4x^{j+k} = 2(V_{j+k} + \delta U_{j+k}), \\
(V_j - \delta U_j) \cdot (V_k - \delta U_k) &= 4(a - x)^{j+k} = 2(V_{j+k} - \delta U_{j+k}).
\end{align*}
\]

Adding these equations yields

\[
2V_{j+k} = V_j V_k + \Delta U_j U_k.
\] (7)

Backwards reading of the recurrence relation leads to \(b^k U_{-k} = -U_k\) und \(b^k V_{-k} = V_k\). Substituting this in equation (7) gives

\[
2b^k V_{j-k} = V_j V_k - \Delta U_j U_k \quad (8)
\]

Putting \(k = j\) yields \(V_j^2 - \Delta U_j^2 = 4b^j\). From (7) we get for \(k = j\) the identity \(2V_{2j} = V_j^2 + \Delta U_j^2\). Adding the last two equations leads to \(V_{2j} = V_j^2 - 2b^j\). Putting \(j := 2j\) the definition (5) gives

\[
W_{2j} \equiv W_j^2 - 2 \pmod{n}
\] (9)

To derive a formula for \(W_{2j+1}\), subtract equation (8) from (7) and get \(V_{j+k} = V_j V_k - b^k V_{j-k}\). Here we take two adjacent even numbers, i.e. we put \(j := 2j+2\) and \(k := 2j\) and get \(V_{4j+2} = V_{2j} V_{2j+2} - b^2 V_2\) in terms of the \(W\)-sequence (5) this is:

\[
W_{2j+1} \equiv W_j W_{j+1} - W_1 \pmod{n}
\] (10)

To compute for a given index \(j \in \mathbb{N}\) the value \(W_j\) write \(j\) in binary, say \(j = (b_0 b_1 \ldots b_k)_2\). Now go through all bits and compute the sequence of pairs \(S_i = \{A, B\} \ (i \geq 0)\)

\[
S_i = \{A, B\} \rightarrow S_{i+1} := \begin{cases} 
\{A^2 - 2, AB - W_1\} \pmod{n} & \text{if } b_{i+1} = 0 \\
\{AB - W_1, B^2 - 2\} \pmod{n} & \text{if } b_{i+1} = 1
\end{cases}
\] (11)

Initialising \(S_0 := \{W_0, W_1\}\) one gets with the pair \(S_k\) exactly the values \(W_j\) und \(W_{j+1}\). So the sequence \((W_j)\) can be computed in a time \(\tilde{O}(\log n)\).

The sequence \((W_j)\) shall now be used for the Lucas test. Let \(a\) be Lucas pseudoprime. Let \(m := (n - (\frac{a}{n}))/2\). Then we get \(U_{2m} \equiv 0 \pmod{n}\). Putting \(j := 2m\), \(k := 2\) in formula (7), it follows \(2V_{2m+2} = \)
\[ V_{2m}V_2 + \Delta U_{2m}U_2 \] Since \( \gcd(b, n) = 1 \) it follows by (5): \[ 2W_{m+1} \equiv W_m W_1 + b^{-(m+1)} \Delta U_{2m}U_2 \quad \text{(mod n)} \] But since \( n \) is Lucas pseudoprime, we get \[ 2W_{m+1} \equiv W_m W_1 \quad \text{(mod n)} \] Since \( \gcd(ab\Delta, n) = 1 \) the converse also holds.

To summarize:

**Theorem 7.** Let \( n, a, b, \Delta, m \) and the sequence \((W_j)\) defined as above. Then \( n \) is Lucas pseudoprime if and only if \[ 2W_{m+1} \equiv W_1 W_m \quad \text{(mod n)} \] Let now \( n \in \mathbb{N}_{\geq 3} \) be a number, that fullfills the assumptions of Definition 3. Then the Frobenius test can be easily implemented using the sequence \((W_j)\). This sequence can be used for the Frobenius test, since from \( \gcd(2\Delta, n) = 1 \) follows, that \( n - (\frac{\Delta}{n}) = 2m \) is even. Clearly Theorem 7 can be used, to test if \( n \) is Lucas pseudoprime. We need a congruence in terms of the sequence \((W_j)\), that is equivalent to the fact

\[ V_{n-(\frac{\Delta}{n})} \equiv \begin{cases} 2b \pmod{n} & \text{if } (\frac{\Delta}{n}) = -1 \\ 2 \pmod{n} & \text{if } (\frac{\Delta}{n}) = 1 \end{cases} \]

Let now \( n \) be Frobenius pseudoprime and \( m = \frac{n - (\frac{\Delta}{n})}{2} \). Then from the definition of the sequence \((W_j)\) we get \[ W_m \equiv 2b^{-(n-1)/2} \quad \text{(mod n)} \] Putting \( B := b^{(n-1)/2} \), it follows \[ BW_m \equiv 2 \pmod{n} \]

To summarize we get the following theorem:

**Theorem 8.** Let \( n, a, b, \Delta, m \) and the sequence \((W_j)\) defined as above. Then \( n \) is Frobenius pseudoprime if and only if \[ 2W_{m+1} \neq W_1 W_m \quad \text{(mod n)} \] and \[ BW_m \equiv 2 \pmod{n} \], \( B = b^{(n-1)/2} \).

**References**

[CrPo05] Richard Crandall, Carl Pomerance, Prime Numbers – A Computational Perspective, Springer, 2005

